



IoT and SCADA Breaches – Bibliography List:

1. Pacemakers patched against potentially lifethreatening hacks. **Link:** nakedsecurity.sophos.com
2. The Industrial Internet of Things and its legal dilemmas. **Link:** gamingtechlaw.com
3. In 2000 major SCADA attack on Australian vendor controlling sewage; leak of 800K liters of raw sewage. **Link to PDF:** pdfs.semanticscholar.org
4. Cyberwar for Sale. **Link:** nytimes.com
5. 5 Industries That Will Be Completely Transformed by IoT. **Link:** hpematter.com
6. Industry Experts' Top IoT Predictions for 2017 and Beyond. **Link:** hpematter.com
7. Futurists Explain Why Technology Will 'Disappear' in 2030. **Link:** hpematter.com
8. 7 tendencias de Internet de las cosas en 2017. **Link:** bbvaopenmind.com
9. The Spy, sorry, The Fridge Who Loved Me. **Link:** nakedsecurity.sophos.com
10. Saudi Arabia Blames Iran For Serious Cyber Attacks. **Link:** oilprice.com
11. Chen, T M and S Abu-Nimeh. "Lessons From Stuxnet". Computer 44, no. 4 (2011): 91-93. Accessed December 22, 2016. **Link:** apus.edu
12. Langner, Ralph. "Stuxnet: Dissecting A Cyberwarfare Weapon". IEEE Security & Privacy Magazine 9, no. 3 (2011): 49-51. Accessed December 2016. **Link:** ieeexplore.ieee.org
13. Schneier, Bruce. "The Story Behind The Stuxnet Virus." Forbes. October 7, 2010. Accessed December 22, 2016. **Link:** forbes.com
14. Ellen Nakashima (2 June 2012). Stuxnet was work of U.S. and Israeli experts, officials say. The Washington Post. Accessed 22 December 2016
15. Broad, William J.; Markoff, John; Sanger, David E. (15 January 2011). Israel Tests on Worm Called Crucial in Iran Nuclear Delay. New York Times. Accessed 22 December 2016
16. Fildes, Jonathan (23 September 2010). Stuxnet worm 'targeted high-value Iranian assets. BBC News. Accessed 22 December 2016
17. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," Survival 53, no. 1 (February – March 2011): 23, doi: 10.1080/00396338.2011.555586.

Contact Us:

TAL Global Worldwide Headquarters:

TAL Global Corporation, 1999 S. Bascom Ave., Suite 925, Campbell, CA 95008, USA

Tel: 408.993.1300; **Fax:** 408.271.9400; **Email:** info@talglobal.net; **Web:** talglobal.com



IoT and SCADA Breaches – Bibliography List:

18. David C. Gompert & Martin Libicki, "Waging Cyber War the American Way," Survival 57, no. 4 (2015): 8, doi: 10.1080/00396338.2015.1068551.
19. AFP. 2016. "NSA Chief Worries About Cyber Attack on US Infrastructure." SecurityWeek, . Web. 24 Dec. 2016. **Link:** securityweek.com
20. Pacemaker data used to help indict alleged arsonist. **Link:** nakedsecurity.sophos.com
21. The easy way your "smart" coffee machine could get hacked and ruin your life. **Link:** qz.com
22. JTAG and UART still good attack vectors: **Link:** praetorian.com
23. IoT Threat environment; Cisco: **Link to PDF:** cisco.com
24. The Threat From Weaponized IoT Devices: It's Bigger Than You Think! **Link:** securityintelligence.com
25. Intel Security chief warns IoT can open up new landscape of attack vectors for future hackers. **Link:** ibtimes.co.uk
26. Getting Your IoT Strategy Right - Learnings From Early Adopters. **Link:** hcltech.com
27. Internet of Things – New security and privacy challenges. **Link:** researchgate.net
28. 4 critical security challenges facing IoT. **Link:** cio.com
29. IoT in Higher Education. **Link:** utdallas.edu
30. The legal considerations of the internet of things. **Link:** computerweekly.com
31. IoT Raises New Legal Challenges For Business. **Link:** informationweek.com
32. Top 5 Legal Issues In The Internet Of Things, Part 1: Data Security & Privacy. **Link:** wassom.com
33. The "Internet of Things" – What is it and what are the legal issues?. **Link:** wriothassall.co.uk
34. IoT Denial of Service Botnets and SCADA Attacks to Plague 2017. **Link:** infosecurity-magazine.com
35. Internet of Things (IoT) Market Trends. **Link:** strategyr.com
36. Harbor Research: The Top 18 IoT Trends to Watch in 2016. **Link:** harborresearch.com
37. Roundup Of Internet Of Things Forecasts And Market Estimates, 2016. **Link:** forbes.com
38. Disney's G-Force 3D Movie Trailer 2009. Link to YouTube Video: youtube.com

Contact Us:

TAL Global Worldwide Headquarters:

TAL Global Corporation, 1999 S. Bascom Ave., Suite 925, Campbell, CA 95008, USA

Tel: 408.993.1300; **Fax:** 408.271.9400; **Email:** info@talglobal.net; **Web:** talglobal.com